Комп'ютерні віруси та антивірусні програмні засоби

Комп'ютерний вірус

- Комп'ютерний вірус — комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Походження терміну

- Назва програми "комп'ютерний вірус" походить від однойменного терміну з біології за її здатність до саморозмноження. Саме поняття "комп'ютерного вірусу" з'явилося на початку 1970-тих і використовувалося у програмуванні та літературі, зокрема, у фантастичному оповіданні "Людина в рубцях" Грегорі Белфорда. Проте, автором терміну вважається Ф. Коен, який у 1984-тому році опублікував одну з перших академічніх статей, що були присвячені вірусам, де і було використано цю назву.

Суспільний аспект

- Для одних віруси є бізнесом. Причому не тільки для їхніх авторів, але і для тих, хто з цими вірусами бореться. Бо процвітання компаній, які випускають антивірусні програми не є несподіванкою ні для кого. Для інших — це хоббі. Хоббі — збирання вірусних колекцій і хоббі — написання вірусів. Ще інші — створюють віруси для прояву власної зухвалості і незалежності, у деяких колах подібна діяльність просто необхідна для підняття свого престижу. Є й такі, для кого віруси це витвір мистецтва; зустрічаються ж лікарі за покликанням, це значить, може бути і комп'ютерний лікар за покликанням. Для деяких віруси служать приводом пофілософствувати, на теми створення і розвитку комп'ютерного життя. Для інших віруси — це також стаття кримінального кодексу. Але для більшості користувачів комп'ютерів віруси — це щоденна головна біль і турбота, причина збоїв в роботі комп'ютера і ворог номер один.

Класифікація комп'ютерних вірусів

За об'єктам, які вражаються:

- файлові віруси
- завантажувальні віруси
- анти-антивірусні віруси
- скриптові віруси
- макро-віруси
- мережеві черв'яки

За способом зараження:

- перезаписуючі віруси
- віруси-компаньйони
- файлові хробаки
- віруси-ланки
- паразитичні віруси
- віруси, що вражають вихідний код программ

За операційними системами і платформами, які вражаються

- DOS
- Microsoft Windows
- Unix
- Linux
- інші

За активностю:

- резидентні віруси
- нерезидентні віруси

За технологіями, які використовуються вірусом:

- нешифровані віруси
- шифровані віруси
- поліморфні віруси
- стелс-віруси (руткіт і буткіт)

За деструктивними можливостями:

- нешкідливі віруси
- безпечні віруси
- небезпечні віруси віруси
- дуже небезпечні віруси

За мовою, на якій написаний вірус:

- асемблер
- високорівнева мова програмування
- скриптова мова

Ознаки зараження вірусом

- Зменшення вільної пам'яті
- Уповільнення роботи комп'ютера
- Затримки при виконанні програм
- Незрозумілі зміни в файлах
- Зміна дати модифікації файлів без причини
- Незрозумілі помилки Write-protection
- Помилки при інсталяції і запуску Windows
- Відключення 32-розрядного допуску до диску
- Неспроможність зберігати документи Word в інші каталоги, крім Template
- Погана робота дисків
- Файли невідомого походження

Ознаки зараження вірусом

- Зникнення файлів
- Форматування HDD
- Неспроможність завантажити комп'ютер
- Неспроможність завантажити файли
- Незрозумілі системні повідомлення, звукові ефекти і т. д.

- Руткіт
- Буткіт
- Методи поширення

- Методи, що перехоплюються сторонніми ПЗ:
- Direct Input
- Full Screen
- OLE
- Прямий доступ до диска (hdo)
- Зміна критичних значень реєстру

- Обмеження функціонування вірусного ПЗ, що накладаються архітектурою ОС.

Антивірусні програми

- Антивірусна програма — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом.

Методи знаходження вірусів

- Антивірусне програмне забезпечення зазвичай використовує два різних методи для виконання своїх задач:
- Перегляд (сканування) файлів для пошуку відомих вірусів, що відповідають визначенню в словнику вірусів.
- Знаходження підозрілої поведінки будь-якої з програм, що схожа на поведінку зараженої програми.

Відповідність визначенню вірусів в словнику

- При цьому методі антивірусна програма під час перегляду файлу звертається до словника з відомими вірусами, що складений авторами програми-антивірусу. У разі відповідності якоїсь ділянки коду програми, що проглядається, відомому коду (сигнатурі) вірусу в словнику, програма-антивірус може виконувати одну з наступних дій:
- Видалити інфікований файл
- Відправити файл у карантин (тобто зробити його недоступним для виконання, з метою недопущення подальшого розповсюдження вірусу).
- Намагатися відтворити файл, видаливши сам вірус з тіла файлу.

Підозріла поведінка програм

- Антивіруси, що використовують метод знаходження підозрілої поведінки програм, не намагаються ідентифікувати відомі віруси, замість цього вони стежать за поведінкою всіх програм. Якщо програма намагається записати якісь дані в файл, що виконується(exe — файл), програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити.

Емуляція (sandbox)

- Деякі програми-антивіруси намагаються імітувати початок виконання коду кожної нової програми, що викликається для виконання, перед тим, як передати їй керування. Якщо програма використовує код, що змінюється самостійно, або проявляє себе як вірус (тобто починає шукати інші exe-файли, наприклад), — така програма буде вважатися шкідливою (здатною нашкодити іншим файлам). Однак цей метод також має велику кількість помилкових попереджень.